Media Protection System and Method and Hardware Decryption Module Used Therein

Abstract

In a media protection system and method, an original media item is encrypted before it is distributed. A digital encryption key for the media item is stored on the consumer's personal smart token. To play the media item, the user inserts the media item into his player along with his smart token, and the digital encryption key is extracted by a hardware decryption module (HDM) in the player (or host device), and is used to determine that the decryption key is linked to the HDM. Once that determination is made, the HDM decrypts the media item as it is played. The HDM provides a USB or other standard interface between a plug connected to the player (or host device) and a socket which receives the smart token. The HDM comprises a decryption processor, a control processor, an internal memory, an external interface, and a memory element, such as a read-only memory (ROM). The HDM is implemented as a self-contained, tamperproof subsystem of the media protection system with which it is associated.